Information and Knowledge Management
ISSN 2224-5758 (Paper) ISSN 2224-896X (Online)
Vol 2, No.1, 2012

A Review of the Underlying Concepts of Electronic Voting

Okediran Oladotun Olusola, Omidiora Elijah Olusayo, Olabiyisi Stephen Olatunde,
Ganiyu Rafiu Adesina
Department of Computer Science & Engineering,
Ladoke Akintola University of Technology, P.M. B. 4000, Ogbomoso, Nigeria

Abstract

Elections and voting are fundamental to any consensus-based society. They are one of the most critical functions of democracy. There are a number of voting systems adopted all over the world with each of them having its peculiar problems. The manual voting system still appears prominent among the developed and developing nations, but with considerations being given to an electronic alternative with a view to showing most of the short comings. Furthermore, with the increased interest and attention on e-government, e-democracy and e-governance, e-voting initiatives have gained more significance. Thus, many countries are piloting with various e-voting models and systems in order to enable voting from anywhere; also, international organisations are developing standards and recommendations in this area. This paper details a review of the underlying concepts of e-voting and discusses some of the salient issues on the subject. Also, a review of common e-voting models, existing elections schemes and explanation of the usual terminologies associated with e-voting were presented.

KEYWORDS: voting, election, democracy, e-voting, cryptography

1. Introduction

Electronic voting has been attracting considerable attention during the last years. The interest in e-voting is based on one hand upon interest and attention devoted to e-government, e-democracy, e-governance, etc. On the other hand, interest in e-voting is founded in problems with conventional election systems. The term e-voting is being used from casting the vote by electronic means to asking the internet community for an opinion on a political issue, as well as from tabulating the votes by electronic means to integrated electronic systems from voters' and candidates' registration to the publication of election results (Buchsbaum, 2004). Other terms, like e.g. e-elections and i-voting have been introduced in order to clarify the specific contents of e-voting. The term e-voting should encompass only political elections and referenda, not initiatives or opinion polls or selective citizens' participation between elections or referenda (e-consultations) (Buchsbaum, 2004).

In general, two main types of e-voting can be identified: e-voting supervised by the physical presence of representatives of governmental or independent electoral authorities, e.g. electronic voting machines at poll sites popularly known as Direct Recording Electronics (DRE); and e-voting within the voter's sole influence (remote e-voting), not physically supervised by representatives of governmental authorities, e.g. voting from one's own or another person's computer via the internet, by mobile phones (including Short Message Service, SMS), or via digital television (Okediran *et al.*, 2011). By this summary categorisation, advance voting of some Nordic countries at postal offices, or kiosk voting at municipal offices can fall, according to specific circumstances, in both of the above cases.

Exhaustive studies have shown that electronic voting, if carefully designed, enhances polling and votes' security, confidentiality, sincerity and increased cost savings on reduced manpower, logistical materials and tools; and above all instant analysis and reporting. Electronic voting further enhances accuracy of all valid votes and final outcome; permit voting once for only eligible voters; allow independent verification of all voters; it can also improve voters' turnaround as it flexibly allows a voter to login and vote from any workstation (Alan, 2005). Therefore, electronic based voting technologies would expand the reach and range of potential voting population.

The rest of the paper is organized as follows; the next section describes the motivation and criteria for electronic voting. Section three presents an apt description of e-voting process while section four discussed some generic cryptographic models for secure electronic voting as proposed by academic literature. Finally, the paper concludes in section five.

2. Motivation and Criteria for Electronic Voting

The right of individuals to vote for their choice representatives is the heart of any democracy. Democracy and elections have more than 2500 years of tradition (Krimmer *et al.*, 2007). However, technology has always influenced and shaped the ways elections are held (Held, 2006). In times past, different voting systems that are based on traditional paper ballots, mechanical devices, or electronic ballots were developed for elections (NSF, 2001) and (Malkawi *et al.*, 2009). However, these voting systems have littered history with example of elections being manipulated in order to influence their outcome. Allegations of violence, intimidation, ballot stuffing, under-age and multiple voting, counting error, complicity of the security agencies and the absence or late arrival of election materials etc often trail elections conducted using these systems of voting (NSF, 2001; Muir *et al*., 2005; Boniface, 2008; Malkawi *et al*., 2009; Okediran *et.al*, 2011).

E-voting is emerging is significant alternative to these conventional systems. The

emergence of e-voting will undoubtedly enable voters to cast their vote from a place other than the poll site in their voting district, facilitate the casting of the vote by the voter, facilitate the participation in elections by those who are entitled to vote, widen access to the voting process for voters with disabilities or those having other difficulties in being physically present at a poll site, increased voter turnout by providing additional voting channels, reduce over time, the overall cost to the electoral authorities of conducting an election, deliver voting results reliably and more quickly amongst many other benefits (Okediran *et al.*,2011).

CoE (2003) recommended that e-voting systems should guarantee the following major principles of democratic elections:

i. Direct suffrage
ii. Universal
iii. Equal
iv. Free
v. Secret

In addition to the aforementioned principles above, (Cranor and Cytron, 1996) and (Lebre *et al.*, 2004) proposed that any electronic voting system should have four core properties that include accuracy, democracy, privacy and verifiability. These four core properties are defined as follows (Cranor and Cytron, 1996):

i. **Accuracy:** A system is accurate if
    a) It is not possible for a vote to be altered,
    b) It is not possible for a validated vote to be eliminated from the final tally, and
    c) It is not possible for an invalid vote to be counted in the final tally.

In the most accurate systems the final vote tally must be perfect, either because no inaccuracies can be introduced or because all inaccuracies introduced can be detected and corrected. Partially accurate systems can detect but not necessarily correct inaccuracies. Accuracy can be measured in terms of the margin of error, the probability of error, or the number of points at which error can be introduced (Cranor and Cytron, 1996).

ii. **Democracy:** Democracy: A system is democratic if
    a) It permits only eligible voters to vote,
    b) It ensures that each eligible voter can vote only once (Cranor and Cytron, 1996).

iii. **Privacy:** A system is private if

a) Neither election authorities nor anyone else can link any ballot to the voter who cast it, and
b) No voter can prove that he or she voted in a particular way.

The second privacy factor is important for the prevention of vote buying and extortion. Voters can only sell their votes if they are able to prove to the buyer that they actually voted according to the buyer's wishes. Likewise, those who use extortion to force voters to vote in a particular way cannot succeed unless they can demand that voters prove that they voted as requested (Cranor and Cytron, 1996).

iv. **Verifiability:** A system is verifiable if voters can independently verify that their votes have been counted correctly.

The most verifiable systems allow all voters to verify their votes and correct any mistakes they might and without sacrificing privacy. Less verifiable systems might allow mistakes to be pointed out, but not corrected or might allow verification of the process by party representatives but not by individual voters (Cranor and Cytron, 1996).

3. Description of the E-voting process

In most election processes, the voting system is always a relatively small part of the whole election process. Generally, an e-voting system consists of six main phases which includes
(Magi, 2007):

- Voters' registration is a phase to define voters for the e-voting system and give them authentication data to log into the e-voting system.
- The authentication is a phase to verify that the voters have access rights and franchise.
- The voting and vote's saving is a phase where eligible voters cast votes and e-voting system saves the received votes from voters.
- The votes' managing is a phase in which votes are managed, sorted and prepared for counting.
- The votes' counting is the phase to decrypt and count the votes and to output the final tally.
- The auditing is a phase to check that eligible voters were capable to vote and their votes participate in the computation of final tally.

From another perspective, Organization for the Advancement of Structured Information Standards (OASIS) described a conceptual perspective of e-voting to be made of three phases namely pre-voting phase, voting phase and post-voting phase. They specified what they called an Election Markup Language (EML) which was designed especially for the exchange of data within e-voting processes. OASIS drafted a high level overview and a high level model dealing with the human view and a high level model dealing with the technical view. These models should be the initial point of creating e-voting concepts. EML is in particular useful for interoperability reasons (Oasis, 2003).

The activities of the pre-voting phase are (Oasis, 2003):

i. Candidate Nomination Process
   a) Candidate Nomination
   b) Candidate Response
   c) Generation of the Candidates List

ii. Voter Registration Process
   a) Voter Registration
   b) Generation of the Election List

Figure 1 depicts the Human Model stated by the Election Markup Language.
The voting phase enables all eligible voters to make their decisions and cast their votes. Thus, by the use of the election list the voter has to authenticate himself/herself as an eligible voter and he/she has to cast his/her individual vote. The model in the figure above does not limit voting on electronic voting only. It is the voters' decision which channel they preferred to cast their ballot. Since the voter should have an alternative to e-voting and since conventional voting with paper ballots must be provided in parallel, the model has to consider multiple possibilities. Especially the interfaces and cutting edges between electronic and conventional elections have to be considered in the conceptional design.

The post-voting phase concerns mainly:

i. Vote counting and
ii. Result reporting

Beside the phases mentioned above, there are some other important parts and elements in the model. Very important are the audit mechanisms needed along all phases of an election. On the one hand, it is important to have possibilities to prove the correctness of the process as such. On the other hand, it is crucial to do not violate the main principles and security requirements, keeping a vote an inviolable secret in particular. However, audit is necessary to prove the authenticity of the result of the election. Thus, a special set of persons, e.g. election officials and candidate's representatives, should be allowed to gain access to auditing information.

System administration is critical as well, since administrators are allowed to access the system. Nevertheless, administration is necessary and therefore the security concept of the e-voting system has to protect critical data and components, the secrecy of the ballots especially. This affects the organizational aspects of the security concept either. Not only technical security mechanisms can guarantee this. The administrative staff has to be elected in respect to reliability as well.

4. Generic Cryptographic Models for Secure Electronic Voting

Since the first cryptographic protocols for electronic elections was published (Chaum, 1981), (Demillo *et al*., 1982; Benaloh, 1987), several solutions have been described in academia to deal with the security problems in online voting. In this section we review three generic models proposed in academic literature for secure e-voting.

4.1 The Mix-net Model

Mix networks (mix-nets), introduced in (Chaum,1981), usually consist of a set of servers (mixes) which accept a batch of input messages and output the batch in randomly permuted (mixed) order so that the input and output messages are unlinkable. Figure 2 depicts then general case of voting with mix-net model. Although originally proposed for anonymous e-mail communication between distrusting entities, mix-nets in online elections aim at hiding the origin of a ballot: tallying officials permute and randomize the encrypted ballots so that the link between the identity of the voter and the vote is broken. Depending on the mixing mechanism, mix-nets can be classified into re-encryption mix-nets and decryption mix-nets.

4.2 The Homomorphic Model

According to this model, introduced in (Cramer *et al.*, 1997) and extended in (Baudron *et al*., 2001), each voter signs and publishes an encryption of his/her vote. Encrypted votes are then “added” into the final tally, to form an encryption of the “sum” of the submitted votes. The model is based on the algebraic homomorphic properties of several probabilistic public key cryptosystems. These cryptosystems encrypt a message *M* by raising a base *g* to the power *M* modulo a large prime number, and then randomizing the result. With homomorphic encryption there is an operation $\oplus$ defined on the message space and an operation $\otimes$ defined on the cipher space, such that the “product” of the encryptions of any two votes is the encryption of the “sum” of the votes, i.e.:

$$EM_1 \oplus EM_2 = E(M_1 \otimes M_2) \quad (1)$$

This property allows either to tally votes as aggregates or to combine shares of votes (Benaloh, 1987; Schoenmakers, 1999), without decrypting single votes. However, each vote must belong to a well-determined set of possible votes such as {+1, -1} for {“yes”, “no”} votes. Moreover, each voter must provide a universally verifiable proof that his/her vote belongs to the predefined set of votes, otherwise, it would be easy for a malicious voter to manipulate the final tally.

After the voting period has closed, a threshold of election authorities cooperatively decrypts the final tally. The results are published on a bulletin board and the accuracy of the voting stage is verified. Depending on the level of trust given to them, the authorities may also provide a publicly verifiable proof that the decryption was correct. In this way individual voters and/or external observers can be assured that all the votes were counted correctly. An example of the homomorphic voting model is shown in Figure 3.

While the original model provides a general framework that allows usage of any probabilistic encryption scheme, only few probabilistic encryption schemes can scale well in large elections with multiple candidates. For example, in (Cramer *et al.*, 1997) a variant of the ElGamal encryption scheme required an exhaustive search over all possible election results by the authorities for the computation of the final tally. Recent proposals have been based on additively homomorphic public key cryptosystems with trapdoor decryption of discrete logarithms (Paillier, 1999; Baudron *et al.*, 2001; Damgard *et al.*, 2003), in order to allow handling of very large tallies.

The homomorphic model satisfies the accuracy, privacy, fairness, robustness and universal verifiability properties. It also inherently supports prevention of double voting, since the voters do not need to be anonymous. It works well in elections where ballots have only questions of a K-out-of-L type, which precludes write-in ballots. Another unattractive feature is that voters may need to run special-purpose code on their computer, for constructing the zero-knowledge proof of validity for their vote.

4.3 The Blind Signature Model

Election protocols of this category, introduced in (Fujioka *et al.*, 1992), enable voters to get their vote validated from an election authority, while preserving the secrecy of their vote. Blind signatures (Chaum, 1982) are the electronic equivalent of signing carbon-paper-lined envelopes: a user seals a slip of a paper inside such an envelope, and later gets it signed on the outside. When the envelope is opened, the slip will bear the carbon image of the signature. When used in an online voting protocol, a voter encrypts, then blinds the vote, and presents it to a validating authority for validation. After the authority validates the vote, the voter un-blinds the encrypted vote and gets a validated vote that cannot longer be correlated to the original blinded message. The voter then uses

an anonymous channel to submit the validated vote to the tallying authorities, as shown in Figure 4.

Protocols within this model are simple, easily manageable, computationally efficient and naturally support “write-in” ballots. A problem with early schemes (Fujioka *et al.*, 1992; Cranor and Cytron, 1996; Herschberg, 1997) was the ability of a malicious server to impersonate absentee voters in the final tally, thus violating the democracy criterion. In the original model (Fujioka et al., 1992) two-phase voting was supported to achieve fairness: voters submitted their encrypted vote and then waited until the end of the election to submit their vote-opening keys. In (Cranor and Cytron, 1997) and (Herschberg, 1997) the protocol of (Fujioka *et al*., 1992) was changed to allow voters to vote and walk away, however in both protocols there is the risk that a malicious authority learns intermediate results, therefore violating the fairness property. In subsequent proposals (Ohkubo *et al.*, 1999; Durette, 1999; Joaquim *et al.*,2003; Lebre *et al.*, 2004) the power of administration is distributed among multiple authorities so that:

i. no election administrator is able to impersonate legitimate voters in the final tally, and
ii. the results are becoming available only at the end of the election.

To establish robustness in the election process, threshold techniques were also proposed (Ohkubo *et al*.,1999; Joaquim *et al*., 2003; Lebre *et al*.,2004). For example, in (Ohkubo *et al*., 1999), a (*t*, *N*) threshold cryptosystem assured that as long as *N-t+1* counters are honest, the results will only be available at the end of the election.

5. Conclusion

In this paper, we gave a short introduction of e-voting system and e-voting systems. We presented the basic requirements and the important assets of electronic elections. A description of the e-voting process was presented and in this course, the Election Markup Language (EML) and the human model given within their definition were presented. We discussed the three main cryptographic schemes for secure electronic voting. These are homomorphic encryption, mixing nets and blind signatures. We provided an explicit description of the core ideas behind these schemes. It is worthy to note that most of the other existing schemes make use of these schemes or a combination of them.

6. References

Alan, D. S. and John, S. C., (2005),” Revolutionalising the Voting Process through Online Strategies, USA Journal on Online Voting Vol. 29, No.5, pp 513-530.

Baudron O., Fouque P., Pointcheval D., Poupard G., and Stern, J., (2001), “ Practical

Multi-
Candidate Election System". In Proc. of the 20th ACM Symposium on Principles of
Distributed Computing. ACM Press, 274–283.

Benaloh J., (1987), "Verifiable Secret Ballot Elections". Ph.D. Thesis, Yale University.

Boniface M., (2008), "A Secure Internet-Based Voting System for Low ICT Resourced Countries". Master of Information Technology Thesis, Department of Information Technology, Makerere University, Uganda.

Buchsbaum T. M., (2004), "E-voting: International Developments and Lessons Learnt". Proceedings of Workshop on Electronic Voting in Europe –Technology, Law, Politics and Society, Austria, at www.subs.emis.de/LNI/Proceedings/Proceedings47/ *Proceeding.GI.47-4.pdf.*

Chaum D., (1981)," Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms".
Communication of ACM 24, 2, 84–88.

Chaum D., (1982)," Blind Signatures for Untraceable Payments". In Proceedings of the Advances in Cryptology – CRYPTO'82. Plenum Press, 199–203.

CoE, (2003)," Council of Europe. Multidisciplinary Ad Hoc Group of Specialists on Legal, Operational and Technical Standards for E-enabled Voting (IP1-S-EE).

Cramer R., Gennaro R., and Schoenmakers B,. (1997), "A Secure and Optimally Efficient Multi-Authority Election Scheme". European Trans. On Telecommunications 8, 5, 481–490.

Cranor L. F. and Cytron R. K., (1996), "Design and Implementation of a Practical Security-
Conscious Electronic Polling System" ,Department of Computer Science, Washington
University St. Louis, Technical Report, WUCS-96-02port.

Damgard I., Jurik M., and Nielsen J., (2003), "A Generalization of Paillier's Public-Key System with Applications To Electronic Voting", International Journal of Information Security to Appear.

Demillo R., Lynch N., and Merritt M., (1982), "Cryptographic Protocols". In Proceedings of the
14th Annual ACM Symposium on Theory of Computing. ACM, 383–400.

Durette, B. W. (1999), ”Multiple Administrators for Electronic Voting. M.S. thesis, Massachusetts Institute of Technology.

ElGamal T. 1985. A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. IEEE Trans. on Information Theory 30, 4, 469–472.

Fujioka A., Okamoto T., and Ohta K. (1992). A Practical Secret Voting Scheme for Large Scale Elections. In Proceedings of the Advances in Cryptology – AUSCRYPT ’92. LNCS, vol. 718. Springer-Verlag, 244–251.

Held D. (2006),” Models of Democracy”, Polity Press, Malden, Cambridge, Third edition.

Herschberg M. (1997). Secure Electronic Voting Using the World Wide Web. M.S. Thesis,
MIT.

Joaquim R., Zuquette, A., and Ferreira P. (2003). REVS - A Robust Electronic Voting.

Krimmer R., Triessnig S. and Volkamer M. (2007), “The Development of Remote E-voting around the World: A Review of Roads and Directions” at http://www.evoting.cc/files/ VOTE-ID-2007/pdf.

Lebre R., Zúquete A. and Ferreira P. (2004),”Internet Voting: Improving Resistance to Malicious Servers in REVS”, IADIS International Conference on Applied Computing
2004, Lisbon, Portugal.

Magi T., (2007),” Practical Security Analysis of E-Voting Systems”, Master of Information
Technology Thesis, Department of Informatics, Tallinn, University of Technology, Estonia.

Malkawi M., Khasawneh M., Al-Jarrah O., (2009), “Modeling and Simulation of a Robust Evoting System”, Communications of the IBIMA, Volume 8, 2009. ISSN: 1943-7765.

Muir H, Laville S. and Gillan A., (2005), "New Fears over Postal Vote Fraud", Accessed at
http://politics.guardian.co.uk/election/story/0,15803,1458341,00.html.

NSF, (2001),” Report on the National Workshop on Internet Voting: Issues and Research

Agenda, National Science Foundation, at http://news.findlaw.com/cnn/docs/voting/ nsfevoterprt.pdf

Oasis, (2003),” Election Markup Language (EML) 4.0a “, Organization for the Advancement of Structured Information Standards”, July 2003.

Ohkubo M., Miura F., Abe M., Fujioka A., and Okamoto T. (1999),” An Improvement on a Practical Secret Voting Scheme”. In Proceedings of the Information Security Conference – IS’99. LNCS, vol. 1729. Springer-Verlag, 225–234.

Okediran O. O., Omidiora E. O., Olabiyisi S. O., Ganiyu R. A., Alo O. O., (2011), “ A Framework for a Multifaceted Electronic Voting System”. International Journal of Applied Science, Philadelphia, USA, vol. 1 No .4 pp 135-142.

Paillier P., (1999), “Public Key Cryptosystems Based On Discrete Logarithms Residues”. In

Proceedings of the Advances in Cryptology – EUROCRYPT’99. LNCS, vol. 1592.

Springer-Verlag.

Schoenmakers B. (1999). A Simple Publicly Verifiable Secret Sharing Scheme and Its Application to Electronic Voting. In Proceedings of the Advances in Cryptology – CRYPTO’99. Vol. 1666.

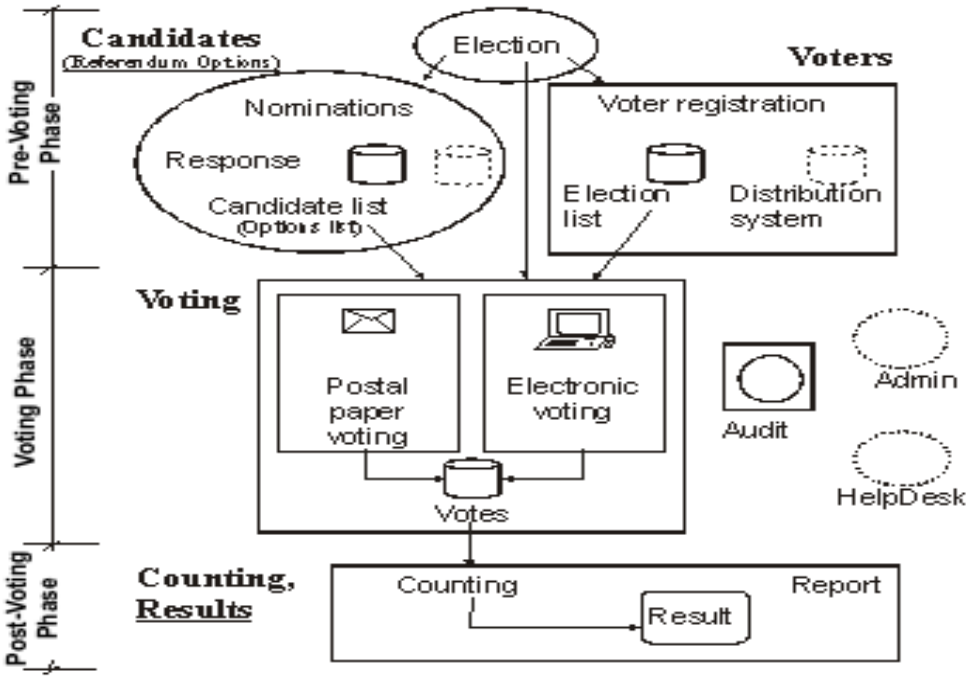

Figure 1: Human Model stated by the Election Markup Language (Oasis, 2003)

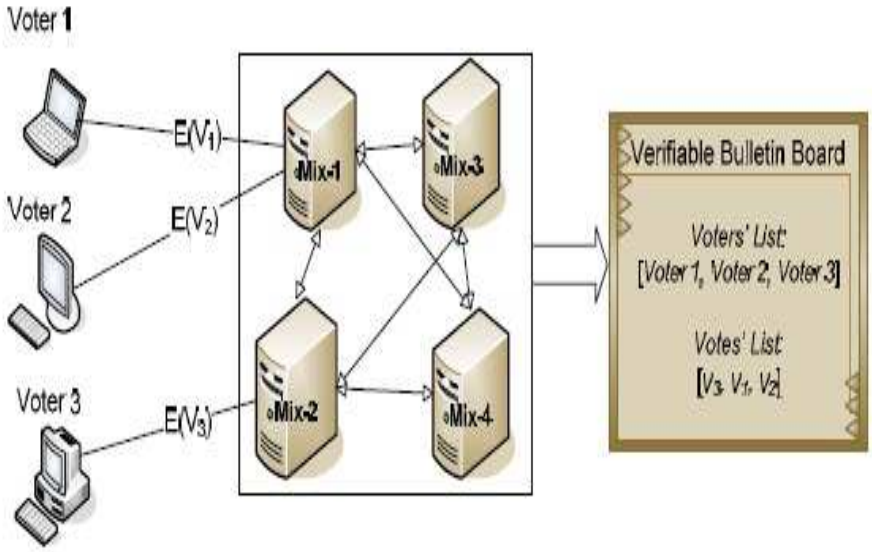

Figure 2: The General Case of Voting with mix-net

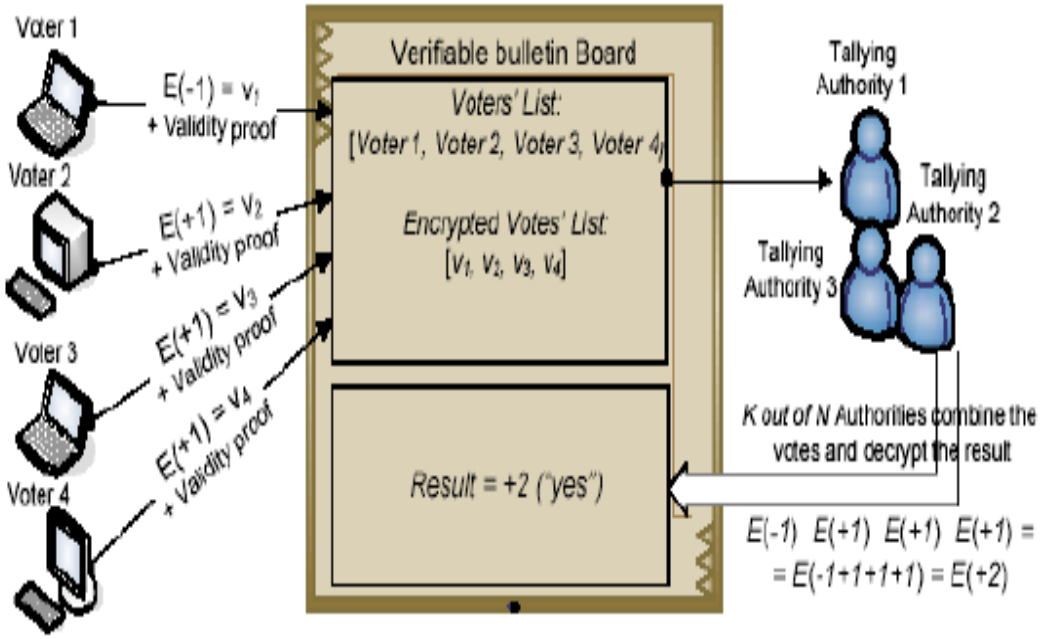

Figure 3: The homomorphic model (Cramer et al., 1997)

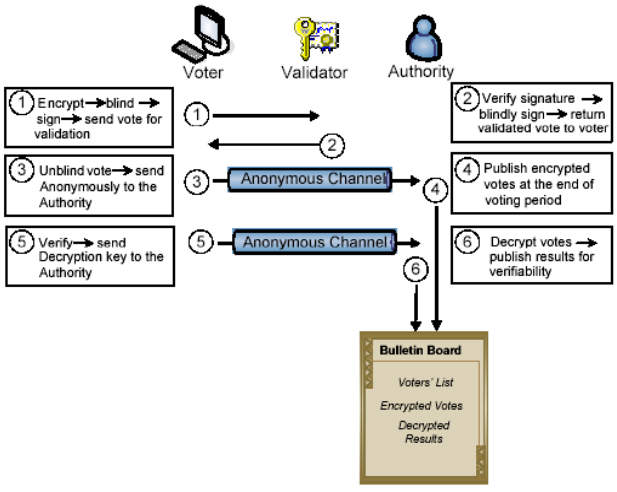

Figure 4: Blind Signature Model (Fujioka *et al*., 1992)